CCIE Security Written Exam v4.0 (350-018)

QUESTION 1
Which two EIGRP packet types are considered to be unreliable packets? (Choose two.)

A. update
B. query
C. reply
D. hello
E. acknowledgement

Answer: DE

QUESTION 2
Before BGP update messages may be sent, a neighbor must stabilize into which neighbor state?

A. Active
B. Idle
C. Connected
D. Established

Answer: D

QUESTION 3
Which three statements are correct when comparing Mobile IPv6 and Mobile IPv4 support? (Choose three.)

A. Mobile IPv6 does not require a foreign agent, but Mobile IPv4 does.
B. Mobile IPv6 supports route optimization as a fundamental part of the protocol; IPv4 requires extensions.
C. Mobile IPv6 and Mobile IPv4 use a directed broadcast approach for home agent address discovery.
D. Mobile IPv6 makes use of its own routing header; Mobile IPv4 uses only IP encapsulation.
E. Mobile IPv6 and Mobile IPv4 use ARP for neighbor discovery.
F. Mobile IPv4 has adopted the use of IPv6 ND.

Answer: ABD

QUESTION 4
Which protocol does 802.1X use between the supplicant and the authenticator to authenticate users who wish to access the network?

A. SNMP
B. TACACS+
C. RADIUS
D. EAP over LAN
E. PPPoE

Answer: D

QUESTION 5
Which two statements are correct regarding the AES encryption algorithm? (Choose two.)

A. It is a FIPS-approved symmetric block cipher.

B. It supports a block size of 128, 192, or 256 bits.
C. It supports a variable length block size from 16 to 448 bits.
D. It supports a cipher key size of 128, 192, or 256 bits.
E. The AES encryption algorithm is based on the presumed difficulty of factoring large integers.

Answer: AD

QUESTION 6
What are two benefits of using IKEv2 instead of IKEv1 when deploying remote-access IPsec VPNs? (Choose two.)

A. IKEv2 supports EAP authentication methods as part of the protocol.
B. IKEv2 inherently supports NAT traversal.
C. IKEv2 messages use random message IDs.
D. The IKEv2 SA plus the IPsec SA can be established in six messages instead of nine messages.
E. All IKEv2 messages are encryption-protected.

Answer: AB

QUESTION 7
DNSSEC was designed to overcome which security limitation of DNS?

A. DNS man-in-the-middle attacks
B. DNS flood attacks
C. DNS fragmentation attacks
D. DNS hash attacks
E. DNS replay attacks
F. DNS violation attacks

Answer: A

QUESTION 8
Which three statements are true about MACsec? (Choose three.)

A. It supports GCM modes of AES and 3DES.
B. It is defined under IEEE 802.1AE.
C. It provides hop-by-hop encryption at Layer 2.
D. MACsec expects a strict order of frames to prevent anti-replay.
E. MKA is used for session and encryption key management.
F. It uses EAP PACs to distribute encryption keys.

Answer: BCE

QUESTION 9
Which SSL protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment?

A. SSL Handshake Protocol
B. SSL Alert Protocol

C. SSL Record Protocol
D. SSL Change CipherSpec Protocol

Answer: C

QUESTION 10
IPsec SAs can be applied as a security mechanism for which three options? (Choose three.)

A. Send
B. Mobile IPv6
C. site-to-site virtual interfaces
D. OSPFv3
E. CAPWAP
F. LWAPP

Answer: BCD

QUESTION 11
Which four options are valid EAP mechanisms to be used with WPA2? (Choose four.)

A. PEAP
B. EAP-TLS
C. EAP-FAST
D. EAP-TTLS
E. EAPOL
F. EAP-RADIUS
G. EAP-MD5

Answer: ABCD

QUESTION 12
According to OWASP guidelines, what is the recommended method to prevent cross-site request forgery?

A. Allow only POST requests.
B. Mark all cookies as HTTP only.
C. Use per-session challenge tokens in links within your web application.
D. Always use the "secure" attribute for cookies.
E. Require strong passwords.

Answer: C

QUESTION 13
Which option is used to collect wireless traffic passively, for the purposes of eavesdropping or information gathering?

A. network taps
B. repeater Access Points
C. wireless sniffers
D. intrusion prevention systems

Answer: C

QUESTION 14
Which traffic class is defined for non-business-relevant applications and receives any bandwidth that remains after QoS policies have been applied?

A. scavenger class
B. best effort
C. discard eligible
D. priority queued

Answer: A

QUESTION 15
In the context of a botnet, what is true regarding a command and control server?

A. It can launch an attack using IRC or Twitter.
B. It is another name for a zombie.
C. It is used to generate a worm.
D. It sends the command to the botnets via adware.

Answer: A

QUESTION 16
Which option is used for anti-replay prevention in a Cisco IOS IPsec implementation?

A. session token
B. one-time password
C. time stamps
D. sequence number
E. nonce

Answer: D

QUESTION 17
Which Cisco ASA feature can be used to update non-compliant antivirus/antispyware definition files on an AnyConnect client?

A. dynamic access policies
B. dynamic access policies with Host Scan and advanced endpoint assessment
C. Cisco Secure Desktop
D. advanced endpoint assessment

Answer: B

QUESTION 18
An attacker configures an access point to broadcast the same SSID that is used at a public hot-spot, and launches a deauthentication attack against the clients that are connected to the hot-spot, with the hope that the clients will then associate to the AP of the attacker.
In addition to the deauthentication attack, what attack has been launched?

A. man-in-the-middle
B. MAC spoofing
C. Layer 1 DoS
D. disassociation attack

Answer: A

QUESTION 19
Which statement best describes the concepts of rootkits and privilege escalation?

A. Rootkits propagate themselves.
B. Privilege escalation is the result of a rootkit.
C. Rootkits are a result of a privilege escalation.
D. Both of these require a TCP port to gain access.

Answer: B

QUESTION 20
Which multicast capability is not supported by the Cisco ASA appliance?

A. ASA configured as a rendezvous point
B. sending multicast traffic across a VPN tunnel
C. NAT of multicast traffic
D. IGMP forwarding (stub) mode

Answer: B